ODNI/NCSC

Enterprise Performance Management
Training and Assistance Group
Instructor-led Course Descriptions

PLEASE READ:

- *Contractors must provide on-site government support and have Government Supervisor or COTR email ONCIX-Training@dni.gov with concurrence for attendance at time of registration and will be added to the general wait list for the course(s) requested.*

ATTENDANCE POLICY: Students are required to attend all scheduled days of training. Classes will begin promptly at 8:00am so please make sure you are familiar with the course location and that you arrive on time.

Privacy Notice:

The information you provide enables the NCSC Training and Assistance Group (TAG) to process your request to participate in a course. It also enables TAG to respond to your inquiries regarding course completion and academic transcripts, should you require such information at a future time. Records are maintained by course title and date of delivery. No other use is made of information contained in registrants' course request forms. The emergency contact information you provide will be maintained securely and deleted upon course completion.

ICD 704 Personnel Security Course

PURPOSE: This course prepares you to make adjudicative decisions consistent with ICD 704 requirements. We will present approaches to enhance best practices and reciprocity across the Intelligence Community and DoD organizations authorized to grant access and adjudicate for Sensitive Compartmented Information. This is an excellent seminar for security professionals who want to better understand the process behind adjudication decisions.

LENGTH: 5 days / 8:00 – 4:30 (8:00 – 12:30 on Friday)

PREREQ:

- Please review ICD 704 prior to attending course.

ICD 705 Physical Security Course

PURPOSE: The ICD 705 Physical Security Course: Lifecycle of A SCIF will prepare you to implement the requirements of the new ICD 705 series documents (ICD 705; ICS 705-1; ICS 705-2 and the ICD 705 Technical Specifications). The course is designed using a SCIF lifecycle theme:

- Phase I: Threat Definition and Planning
- Phase II: Preliminary Construction Planning
- Phase III: Design and Construction Requirements
- Phase IV: Accreditation
- Phase V: SCIF Operations and Management
- Phase VI: Disposal of a SCIF

The course stresses comprehension and construction best practices and application of the ICD 705 series documents.

LENGTH: 5 days / 8:00 – 4:30 (8:00 – 12:30 on Friday)

PREREQ:

- Please review the following documents prior to course attendance:
  - IC Directive 705, Sensitive Compartmented Information Facilities (SCIFs)
  - IC Standard 705-1, Physical and Technical Standards for SCIFs
  - IC Standard 705-2, Standards for Accreditation and Reciprocal Use of SCIFs

Special Security Officer Course (SSOC)

PURPOSE: Prepare security professionals who administer SCI programs. We use practical implementation exercises to give hands-on experience. The topics include:

- Structure of Intelligence Community
- Security Incidents and Investigations
- Business and Security Interfaces
- Security Awareness, Training, and Education Programs
- Physical Security (ICD 705)
- Personnel Security (ICD 704)
- Information Systems Security (ICD 503)

LENGTH: 5 days / 8:00 – 4:30 (8:00 – 12:30 on Friday)

PREREQ:

- Recommended that they have 2-5 years security experience

INSIDER THREAT **HUB OPERATIONS** COURSE

PURPOSE: This is a new course to introduce and exercise the basic functions of an Insider Threat program's centrally managed analysis and response capability (referred hereinafter as the "Hub") to gather, integrate, analyze, and respond to potential insider threat information derived from counterintelligence, security, information assurance, human resources, law enforcement, and other internal and external sources. This is a practical, scenario-based course designed to expose Insider Threat personnel to realistic events in the day-to-day operations of an Insider Threat Hub. The class will include break out teams with an assigned instructor/facilitator for specialized attention. This course supersedes the previous National Insider Threat Task Force's (NITTF's) "Establishing and Operating an Insider Threat Program", "Principles of Hub Operations: Insider Threat Course", and "Principles of Hub Operations Course". The topics include:

- Insider Threat Program Hub Functions
- Legal Considerations
- Classification of Insider Threat information
- Inquiry fundamentals
- Response actions and Referrals
- Reporting and Documentation concepts

LENGTH: 3 days / 8:00 – 4:30

PREREQ: Insider Threat Program Manager/Senior Official must send e-mail concurrence to ONCIX-Training@dni.gov for participant(s) enrollment at time of registration. Prerequisite training includes CI & Security Awareness Training, and Insider Threat Awareness Training. Prefer participants hold certificates in at least one of previous Insider Threat courses and be familiar with the Insider Threat Security Classification Guide.

OBJECTIVES:

- Understand the functions of Insider Threat Hub Operations
- Describe the policies and processes for Hub functions to effectively gather information
- Understand the legal considerations in establishing information flow processes, and handling information from a variety of internal and external sources
- Demonstrate how to gather and document counterintelligence, security, information assurance, human resource, law enforcement, and other information related to potential Insider Threat activities.
- Demonstrate how to integrate and analyze relevant information on potential Insider Threat activities.
- Demonstrate how to complete plans and reports with recommendations for follow-on actions in response to potential Insider Threat activities.
- Practical Exercises to Reinforce Learning